This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

# Pelta Lumi

## Sistema Distribuido y Evolutivo de Detección de Influencia Digital y Perfilamiento

### Resumen Ejecutivo

**Pelta Lumi** es un sistema distribuido, evolutivo y multimodal de inteligencia artificial cuyo objetivo es detectar, clasificar y notificar al usuario, en tiempo real, sobre mecanismos digitales diseñados para influir en su comportamiento, decisiones de compra, desplazamientos físicos, exposición a contenido y privacidad personal.

El sistema opera bajo tres principios irrenunciables:

1. **Honestidad de cobertura** — distingue Evidencia Directa, Inferencia Probabilística e Hipótesis de Riesgo en cada notificación.
2. **Soberanía del usuario** — procesamiento local por defecto; sin telemetría sin consentimiento explícito.
3. **Inmutabilidad de evidencia** — todos los eventos detectados se registran en logs criptográficamente sellados mediante el **Quantum Hash Framework (QHF)**, exportables para litigio, auditoría o regulación.

A partir de la versión 5.0, el **Immutable Log Store** de Pelta Lumi adopta el QHF como descriptor determinístico de estado, garantizando:

- Huella criptográfica reproducible de cada evento de telemetría.
- Preparación para reemplazar SHA-256/ECDSA por primitivas post-cuánticas (CRYSTALS-Dilithium, SPHINCS+, BLAKE3) sin cambiar la arquitectura del modelo.
- Interoperabilidad con estándares actuales (OpenTelemetry, SIEM/SYSLOG, REST, gRPC) y futura compatibilidad con infraestructura cuántica.

El piloto inicial opera en dispositivos Android, con extensión prevista a iOS, PC, tablet, plataformas web y hardware embebido.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

**Documentos del conjunto:**

- **Pelta Lumi v5.0** (este documento): Arquitectura, módulos técnicos, modelos IA, despliegue y KPIs.
- **Annex A v5.0**: Catálogo completo de vectores de perfilamiento y ataque a la psique humana.
- **Annex B v1.0**: Especificación técnica de integración del Quantum Hash Framework.
- **Annex C v1.0**: Interoperabilidad con sistemas actuales y migración a nuevas tecnologías.

# Parte I — Principios de Diseño

## 1.1 Honestidad de Cobertura y Observabilidad Real

Pelta Lumi opera dentro del espacio de usuario del sistema operativo. Esto impone límites duros que se comunican explícitamente en toda notificación:

**Observable directamente:**

- Uso de permisos auditables por el S.O. (cámara, micrófono, ubicación, contactos, almacenamiento).
- Tráfico de red interceptable mediante VPN local o DNS proxy (metadatos: dominio, frecuencia, volumen, SNI — no payload cifrado).
- Escaneo de señales Bluetooth Low Energy (BLE) y Wi-Fi permitidas por las APIs del sistema.
- Metadatos de aplicaciones instaladas, SDKs embebidos y patrones de uso.
- Patrones de consumo de batería y CPU correlacionables con activaciones de sensores.
- Notificaciones push recibidas, frecuencia, contenido textual (con permiso de accesibilidad) y timing contextual.

**Solo inferible (probabilístico):**

- Co-ubicación de dispositivos a partir de señales BLE/Wi-Fi compartidas.
- Perfilamiento cruzado a partir de SDKs y dominios compartidos entre apps.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

- Influencia en tiempo real sobre decisiones: correlación contextual entre ubicación física, apps activas, notificaciones recibidas y patrones de comportamiento histórico.
- Activaciones sospechosas de sensores (cámara/micrófono sin UI visible, correlacionadas con red).

**Fuera del alcance sin privilegios especiales:**

- Operaciones exclusivas del TEE/TrustZone o firmware de baseband.
- Payload de tráfico cifrado end-to-end.
- Activaciones a nivel de hardware invisibles al kernel de usuario.
- Canales acústicos de vibración (demostrado en laboratorio con ~60% de precisión; fuera del alcance de app estándar sin permiso de audio).

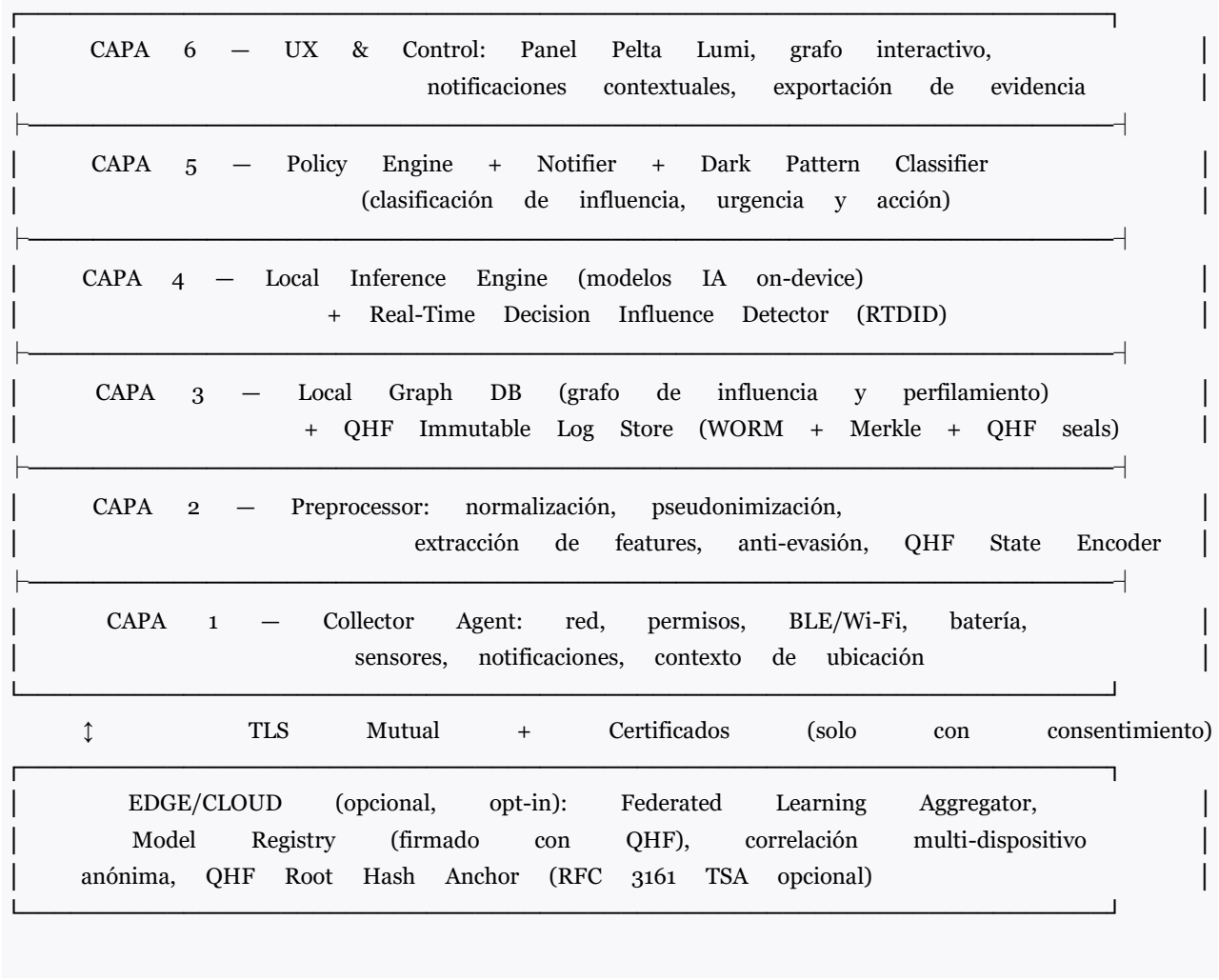
## 1.2 Principios Arquitectónicos

| Principio | Implementación |
|---|---|
| **Privacidad por diseño** | Procesamiento on-device prioritario; telemetría a edge/cloud solo con consentimiento; k-anonymity (k≥5) y differential privacy antes de cualquier exportación |
| **Respuesta en tiempo real** | Detección local <200 ms; notificación al usuario <1 s |
| **Logs inmutables QHF** | Cada evento sellado con descriptor QHF + SHA3-256 (hoy) / BLAKE3 + CRYSTALS-Dilithium (post-cuántico); cadena Merkle verificable; exportable por el usuario |
| **Explicabilidad** | Toda detección incluye: nivel de certeza, evidencia listada, explicación en lenguaje natural, acción recomendada |
| **Defensa adversarial** | Entrenamiento adversarial, detección de distributional shift, umbrales adaptativos por dispositivo |
| **Extensibilidad** | Arquitectura modular; integrable en PC, tablet, navegador, router doméstico, IoT |
| **Preparación cuántica** | Capa criptográfica separada del modelo de datos; migración a NIST PQC sin cambio de esquema (ver Annex B) |

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

## Parte II — Arquitectura General

### 2.1 Capas del Sistema




### 2.2 Integración con Ecosistema Actual

| Protocolo / Estándar | Rol en Pelta Lumi | Interfaz |
|---|---|---|
| **REST / JSON-API (OpenAPI 3.1)** | Exportación de eventos de detección a SIEMs y dashboards | `/api/v1/detections`, `/api/v1/log/export` |

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

| | | |
|---|---|---|
| **gRPC + Protobuf** | Telemetría binaria entre agente on-device y edge aggregator | PeltaLumiTelemetry.proto |
| **OpenTelemetry (OTLP)** | Trazabilidad en infraestructura cloud; compatible con Grafana, Jaeger, Datadog | Exportador OTLP configurable |
| **SIEM / SYSLOG (CEF/LEEF)** | Forwarding de alertas a Splunk, QRadar, Microsoft Sentinel | Transformador eventos QHF → CEF |
| **MDM (Android Enterprise / Apple DEP)** | Despliegue del agente en flotas corporativas | Política MDM de Pelta Lumi Agent |
| **Android Keystore / iOS Secure Enclave** | Almacenamiento HSM-backed de clave de firma del log | Keystore API / CryptoKit |
| **WebAssembly (WASM)** | Verificación portable de log exportable en cualquier navegador | pelta-lumi-verify.wasm |
| **RFC 3161 TSA** | Anclaje de Merkle root en Timestamping Authority externa | Estándar IETF |

## Parte III — Módulos Técnicos

## 3.1 Collector Agent (on-device)

| Fuente | Android | iOS | Condición |
|---|---|---|---|
| AppOps cámara/micrófono | AppOpsManager (API 19+), indicadores Android 12+ | App Privacy Report, indicadores naranja/verde | Con permisos del usuario |
| Tráfico de red (metadatos DNS/TLS) | VPNService local, NetworkStatsManager | NEPacketTunnelProvider | Solo metadatos (dominio, frecuencia, volumen, SNI) |
| Escaneo BLE / Wi-Fi | BluetoothLeScanner, WifiManager | CoreBluetooth, NEHotspotHelper | Con permiso explícito |
| Notificaciones push | NotificationListenerService (con permiso) | Restringido por sandbox | Requiere permiso de accesibilidad en Android |
| Uso de apps | UsageStatsManager | Limitado | Requiere permiso PACKAGE_USAGE_STATS |

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

| | | | |
|---|---|---|---|
| Geofence / contexto de ubicación | Geofencing API, FusedLocationProvider | CoreLocation | Con permiso de ubicación |
| Sensores de movimiento | SensorManager | CoreMotion | Sin permiso especial |
| Consumo de batería / CPU | BatteryManager, PowerManager | Limitado | Proxy para anomalías de activación |

## 3.2 Preprocessor + QHF State Encoder

- Normalización temporal y de features multimodales.
- Pseudonimización: hashing SHA-256 de identificadores de app y dispositivo.
- k-Anonymity local: ningún evento sale del dispositivo que no cumpla k≥5 en su grupo temporal.
- Feature extraction: vectores temporales de red, embeddings de texto, fingerprints de SDK, señales de beacon.
- **QHF State Encoder (NUEVO v5.0):** convierte cada vector de features en la tupla (X_O, S_norm, E_O, T, C, M) compatible con el descriptor QHF, preparándolo para el Immutable Log Store. Ver Annex B para especificación completa.

## 3.3 QHF Immutable Log Store

Cada evento detectado genera un bloque QHF con la siguiente estructura:

```
{
 "block_id": "uuid-v4",
 "sequence": 12345,
 "timestamp": "2026-05-14T20:00:00.000Z",
 "prev_hash": "sha3-256:abc123...",
 "event_hash": "sha3-256:def456...",
 "qhf_descriptor": {
  "X_O": 0.723,
  "S_norm": 0.41,
  "E_O_log10": 7.82,
  "T_index": 12345,
  "C_code": 1,
```

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero


```
  "metadata": {
    "system_class": "mobile_telemetry",
    "protocol": "pelta_lumi_v5",
    "scale_class": "device_event",
    "model_version": "5.0.0"
  }
 },
 "qhf_hash": "sha3-256:qhf789...",
 "qhf_params": {
  "hash_function": "SHA3-256",
  "kappa": 10.0,
  "gamma": 1.0,
  "S_ref": 0.5,
  "S_max": "log_d",
  "serialization": "canonical_json_sorted_keys_utf8"
 },
 "detection_summary": {
  "type": "real_time_influence|cross_profiling|co_location|suspicious_activation|dark_pattern",
  "certainty_level": "evidence|inference|hypothesis",
  "confidence_score": 0.87,
  "confidence_interval_95": [0.81, 0.93],
  "apps_involved": ["app_hash_1", "app_hash_2"],
  "action_taken": "notified|blocked_domain|permission_revoked|logged_only"
 },
 "merkle_root": "sha3-256:ghi789...",
 "signature": {
  "algorithm": "ECDSA-P256",
  "value": "ecdsa:jkl012...",
  "pqc_ready": true,
  "pqc_algorithm_planned": "CRYSTALS-Dilithium-3"
 }
}
```


**Propiedades del log:**

- **Append-only:** ningún proceso puede sobrescribir ni eliminar bloques durante el período de retención (default: 90 días).
- **Detección de tampering:** cualquier modificación rompe la cadena QHF — detectable en <100 ms.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

- **Auditable:** exportación completa en JSON-LD con firma verificable, apto para GDPR/LGPD/CCPA/DSA.
- **Portable:** verificación con `pelta-lumi-verify.wasm` sin instalar Pelta Lumi.

## 3.4 Local Inference Engine

| Modelo | Arquitectura | Uso | Latencia target |
|---|---|---|---|
| Anomalía de sensor | 1D-CNN + TCN + VAE | Activaciones sospechosas de sensores, patrones de red anómalos | <50 ms |
| Grafo de influencia | GAT + GraphSAGE | Comunidades de SDKs, ID bridging, perfilamiento cruzado | <100 ms |
| Dark Pattern Classifier | Transformer ligero + ViT-Tiny | Clasificación de notificaciones push y UIs sospechosas | <80 ms |
| Influencia en tiempo real | Transformer multimodal | Correlación ubicación-app-notificación-beacons | <150 ms |
| Explicabilidad | SHAP / Attention heads | Explicación de detecciones | <50 ms |

## 3.5 Real-Time Decision Influence Detector (RTDID)

Módulo central que detecta cuando el entorno digital está diseñado para influir activamente en una decisión del usuario **en el momento en que esa decisión se está tomando**:

| Vector | Descripción | Certeza |
|---|---|---|
| Geofence trigger | App activa notificación push al cruzar un perímetro virtual GPS/BLE | Evidencia Directa |
| Beacon proximity nudge | Beacon BLE en tienda activa sugerencia de producto en el pasillo | Evidencia Directa |
| Temporal pressure notification | Notificación con contador de tiempo regresivo o urgencia artificial | Inferencia Fuerte |
| Cross-app behavioral trigger | App A (salud) + App B (retail) sincronizan datos en <500 ms | Inferencia Fuerte |
| Personalized dark pattern | UI diseñada para el perfil individual del usuario | Inferencia Fuerte |

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

| | | |
|---|---|---|
| Social proof manipulation | "14 personas viendo este producto ahora" (no verificable) | Inferencia Fuerte |
| Mood/context timing | Push enviada en período de inactividad >20 min (mayor impulsividad) | Inferencia Fuerte |
| Sequential commitment | Microcompromisos incrementales hacia decisión mayor | Hipótesis de Riesgo |
| Consent string manipulation | IAB TCF configurado para maximizar aceptación | Inferencia Fuerte |

## 3.6 Policy Engine y Notifier

| Nivel | Condición | UX |
|---|---|---|
| **EVIDENCIA DIRECTA** | Evento registrado por S.O. + ≥2 señales correlacionadas | ◍ Alerta inmediata, vibración |
| **INFERENCIA FUERTE** | Correlación estadística significativa de múltiples señales | ◍ Notificación destacada |
| **HIPÓTESIS DE RIESGO** | Patrón compatible sin confirmación | ◍ Notificación discreta |
| **INFLUENCIA DETECTADA** | Vector de influencia en tiempo real identificado | ◍ Alerta contextual |
| **INFO / LOG** | Evento registrado sin riesgo inmediato | ◯ Solo en log QHF |

## Parte IV — Catálogo de Vectores

El catálogo completo y científicamente documentado de todos los vectores de perfilamiento psicológico, conductual, biométrico, cognitivo, emocional y de side-channels de hardware, incluyendo referencias científicas, mecanismo técnico y capacidad de detección en Pelta Lumi, se documenta en el **Annex A**.

**Gaps explícitos (fuera del alcance del MVP estándar):**

| Vector | Limitación | Ruta futura |
|---|---|---|
| TEE/TrustZone covert channels | No visible desde espacio de usuario | Forense de firmware o hardware externo |

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

| | | |
|---|---|---|
| Firmware de baseband | Por debajo del kernel de usuario | Fuera del alcance de app estándar |
| Canal acústico de vibración | ~60% de precisión en laboratorio | Contramedidas de hardware |
| Wireless charger side-channel (2026) | Sin software detectable | Hardware externo de análisis electromagnético |
| Ultrasound cross-device (payload) | Requiere permiso de micrófono | Disponible si el usuario otorga permiso de audio (M4) |

## Parte V — Especificación Técnica de Modelos IA

### 5.1 Estrategias de Entrenamiento

- **Federated Learning:** gradientes agregados centralmente sin compartir datos crudos; Secure Aggregation.
- **On-device continual learning:** buffers locales y experience replay controlado; adaptación al comportamiento del usuario sin enviar datos.
- **Meta-learning (MAML-like):** adaptación rápida a nuevas apps o patrones de SDK no vistos durante el entrenamiento.
- **Validación adversarial:** timing obfuscation, beacon spoofing, fingerprint poisoning, SDK carga dinámica.

### 5.2 Datasets de Entrenamiento

- 52 SDKs de scanning inalámbrico en ~10,000 apps Android (IMDEA Networks / PoPETs 2025).
- Dataset Contextico-D: 1,524 UIs móviles con 1,871 instancias de dark patterns en 13 tipos.
- Dataset UIGuard: 4,999 UIs benignas + 1,353 UIs maliciosas de 1,023 apps móviles.
- Dataset SKAID (2025): audio de teclado + logs de teclas para defensa contra keystroke inference.
- Sintéticos: escenarios simulados de geofencing, beacons, co-ubicación y timing de nudges.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

# Parte VI — Robustez y Defensa Adversarial

## 6.1 Pipeline de Verificación de Detecciones

Señal bruta → Detección estadística (modelo IA) → Inferencia causal (Granger/PC)
→ Verificación por evidencia cruzada (≥2 fuentes independientes)
→ Búsqueda de explicaciones alternativas (módulo de falsificabilidad)
→ Clasificación de nivel (Evidencia / Inferencia / Hipótesis)
→ Generación de explicación en lenguaje natural
→ QHF State Encoding + Registro en Immutable Log (bloque sellado)
→ Notificación al usuario (según nivel)

## 6.2 Defensa Adversarial

| Ataque | Defensa |
|---|---|
| Timing obfuscation | Ventanas temporales adaptativas + análisis de distribución estadística |
| Fingerprint poisoning | Ensemble de modelos + monitor de integridad de features |
| Beacon spoofing | Correlación multi-señal obligatoria (BLE + Wi-Fi + DNS) |
| SDK carga dinámica | Análisis de comportamiento en runtime + monitorización de tráfico |
| Exfiltración en lotes pequeños | Análisis acumulativo en ventanas de 24h y 7d |
| Distributional shift | Detección de drift + reentrenamiento federated |
| Modificación del log local | Verificación de cadena QHF hashes; clave de firma en Keystore |
| **Ataque cuántico a ECDSA/SHA-256** | **Migración planificada a CRYSTALS-Dilithium + BLAKE3 (ver Annex B)** |

# Parte VII — Despliegue en Piloto

## 7.1 Android — Plataforma Principal del MVP

| Permiso | Uso | Tipo |
|---|---|---|
| PACKAGE_USAGE_STATS | Monitoreo de uso de apps | Requiere aprobación manual en Ajustes |

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

| | | |
|---|---|---|
| BIND_NOTIFICATION_LISTENER_SERVICE | Análisis de notificaciones push | Requiere aprobación manual |
| BIND_VPN_SERVICE | VPN local para metadatos de red | Requiere confirmación del usuario |
| ACCESS_FINE_LOCATION | Escaneo BLE/Wi-Fi + geofence | Requiere permiso explícito |
| BLUETOOTH_SCAN | Escaneo de beacons BLE | Android 12+ |
| FOREGROUND_SERVICE | Agente en background | Notificación persistente visible |

## 7.2 Extensibilidad

| Plataforma | Mecanismo | Prioridad |
|---|---|---|
| Android | Agente app + VPN local + Keystore + QHF log | MVP |
| iOS | NetworkExtension + CoreBluetooth + MDM | V2 |
| PC Windows | WFP + ETW + QHF log | V2 |
| PC macOS | Network Extension + Endpoint Security | V2 |
| Navegador web | Extensión Chrome/Firefox (dark patterns + TCF) | V2 |
| Router doméstico | OpenWRT / pi-hole plugin + DNS analysis | V3 |
| Wearables | Wear OS / watchOS agent con QHF sync | V3 |
| SIEM corporativo | REST/CEF + QHF hash forwarding | V2 |

## 7.3 Optimización de Batería

- Sampling adaptativo: 1 Hz en modo de riesgo activo; 0.1 Hz en modo reposo.
- Batching de inferencias cada 5-15 s.
- Aceleradores: NNAPI (Android) y CoreML (iOS).
- Freeze de modelos en background cuando batería <15%.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

- **Meta:** impacto <3% de batería por día en uso normal.

## Parte VIII — Plan de Pruebas y KPIs

### 8.1 KPIs del Sistema

| Métrica | Umbral MVP | Justificación |
|---|---|---|
| Precision (Evidencia Directa) | ≥ 0.95 | Falsos positivos dañan credibilidad |
| Precision (Inferencia Fuerte) | ≥ 0.85 | Tolerable con incertidumbre explícita |
| Recall global | ≥ 0.80 | Preferir no perder amenazas reales |
| Precision (Dark Pattern Classifier) | ≥ 0.82 | Benchmark UIGuard |
| F1 (Dark Pattern Classifier) | ≥ 0.85 | Benchmark DPDGPT |
| Latencia detección local | < 200 ms | Tiempo real efectivo |
| Latencia notificación | < 1 s | UX aceptable |
| Datos PII enviados sin consentimiento | 0% | Obligatorio |
| Telemetría enviada agregada | > 95% | Estándar de privacidad |
| Consumo adicional de batería | < 3% / día | Sostenibilidad de uso |
| Integridad de log QHF (tampering rate) | 0% | Verificación de Merkle + QHF chain |
| QHF hash reproducibility | 100% | Determinismo garantizado por QHF |
| Tiempo de detección de tampering en log | < 100 ms | Respuesta inmediata |

### 8.2 Escenarios de Validación

**Escenario A — Perfilamiento directo:** App con micrófono activo sin UI visible + 18 KB a dominio de analytics → EVIDENCIA DIRECTA en <200 ms. Bloque QHF generado y verificable.

**Escenario B — Influencia en tiempo real:** Usuario entra a geofence → beacon BLE → push con urgencia artificial → INFLUENCIA DETECTADA antes de que el usuario abra la notificación.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

**Escenario C — Perfilamiento cruzado:** Dos apps con SDK compartido sincronizan en 400 ms → GNN detecta comunidad y ID bridging → INFERENCIA FUERTE.

**Escenario D — Co-ubicación inferida:** Dispositivo sin GPS + 3 dispositivos con ubicación conocida detectan los mismos beacons → score >0.75 → HIPÓTESIS DE RIESGO con IC 95%.

**Escenario E — Dark pattern:** Banner "Aceptar todo" destacado + rechazo en gris pequeño → consent_manipulation → log QHF registrado como INFERENCIA FUERTE.

**Escenario F — Falso positivo:** App de videoconferencia activa cámara con UI visible → Pelta Lumi NO dispara alerta.

**Escenario G — Integridad QHF:** Modificación de un byte en log local → detección de ruptura de cadena QHF en <100 ms.

**Escenario H — Verificación portable:** Exportación JSON-LD → verificación exitosa con `pelta-lumi-verify.wasm` en navegador sin instalar Pelta Lumi.

## Parte IX — Marco Legal y Regulatorio

**Marcos regulatorios relevantes:**

- **GDPR (Europa):** el consent string IAB TCF ha sido declarado por el TJUE como dato personal. El QHF Immutable Log de Pelta Lumi sirve como evidencia exportable ante autoridades de protección de datos.
- **DSA (Digital Services Act, UE):** prohíbe explícitamente dark patterns que comprometan la libre elección del usuario.
- **LGPD (Brasil), CCPA (California), PIPL (China):** derechos de acceso, portabilidad y oposición facilitados por el log exportable.
- **NIST AI Agent Standards Initiative (EE.UU., 2026):** lineamientos de gobernanza para sistemas de IA autónomos.
- **NIST PQC Standards (FIPS 203/204/205, 2024):** ruta de migración post-cuántica documentada en Annex B.
- **ISO/IEC 27037:** preservación de evidencia digital — compatible con log QHF.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

El log QHF de Pelta Lumi, con su cadena de hashes verificable, firma criptográfica y anclaje RFC 3161 opcional, cumple los requisitos de admisibilidad de evidencia digital en los marcos regulatorios mencionados.

## Conclusión

Pelta Lumi v5.0 es la especificación técnica de un sistema verificable, falsificable, extensible, defendible e interoperable que cubre los vectores de influencia digital y perfilamiento más documentados en la literatura científica y la práctica industrial contemporánea.

Sus cuatro aportaciones principales son:

1. **Detección de influencia en tiempo real sobre decisiones humanas** — especialmente en entornos físico-digitales (retail, movilidad, salud, entretenimiento).
2. **QHF Immutable Log** — logs sellados con el Quantum Hash Framework que convierten cada evento detectado en evidencia criptográficamente verificable, exportable ante autoridades o tribunales, y preparada para migración post-cuántica sin cambio de esquema.
3. **Clasificador de dark patterns** — ejecutado on-device, capaz de identificar manipulación de consentimiento, urgencia artificial y presión social en notificaciones push e interfaces.
4. **Honestidad de cobertura estructural** — la distinción obligatoria entre Evidencia Directa, Inferencia Fuerte e Hipótesis de Riesgo en cada notificación es el mecanismo que hace al sistema científicamente responsable y legalmente defendible.

**LICENSE AND CONDITIONS OF USE.**
The content is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) license:
https://creativecommons.org/licenses/by-nc-sa/4.0/
By using this content and model, you agree to:
Provide appropriate credit, include a link to the above license, and indicate if changes were made.
Not use the material or any derivative works for commercial purposes.
Distribute any adaptations or derivative works only under the same CC BY-NC-SA 4.0 license.
Not apply legal terms or technological measures that legally restrict others from doing anything the license permits.
Data logging and trade secrets policy.
The design, implementation, and deployment of this model, as well as any derivatives, do not authorize the collection, storage, or exploitation of IP addresses, unique device identifiers, or other technical traceability data for commercial profiling, targeted advertising, or any other economic exploitation.
Any system implementing this model must limit the logging and retention of IP addresses and other identifiable data strictly to what is necessary to:

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

(a) maintain technical security and service integrity; and
(b) comply with applicable legal obligations (for example, any minimum log retention required by law).
It is prohibited to use this model or its derivatives to:
capture, store, or exploit trade secrets, proprietary know-how, or confidential information of users or third parties for any purpose other than providing the technical service described in this documentation; or train or improve closed, commercial systems using data that contains confidential information of third parties without their prior, explicit, written consent.

---+EOD+---